Journal of Number Theory **74**, 1–18 (1999)
Article ID jnth.1998.2307, available online at http://www.idealibrary.com on IDEAL®

Twists of Galois Representations and Projective Automorphisms*

Siman Wong

Department of Mathematics, Brown University, Box 1917, Providence, Rhode Island 02906
E-mail: SIMAN@math.brown.edu

Communicated by K. Rubin

Received January 16, 1997; revised May 11, 1998

We show that two surjective λ-adic Galois representations which are λ-adically close near the supersingular primes are equivalent up to a twist and a standard determining the automorphisms of PGL_n over a complete local ring.

1. INTRODUCTION

If two elliptic curves defined over a number field are quadratic twists of each other, then their $a(p)$'s coincide up to sign for almost all p (i.e., all but finitely many). Serre [21, Section 6] showed that the converse also holds, by relating the $a(p)$'s to the trace of Frobenius of the associated l-adic GL_2-representations. Note that the condition $a_1(p) = \pm a_2(p)$ implies that the supersingular primes of the two curves agree up to finitely many exceptions. In this paper we study the analogous problem of determining a λ-adic GL_n-Galois representation up to twists by imposing conditions on a "λ-adic neighborhood of the supersingular primes."

Let $\mathcal{O}$ be a commutative, complete local ring with residue field k and maximal ideal λ. Let K be a finite extension of $\mathbb{Q}$. Let $G_K = \mathrm{Gal}(\bar{K}/K)$, and let $\rho_1, \rho_2 : G_K \to GL_n(\mathcal{O})$ be surjective, continuous Galois representations which are unramified outside a finite set of primes S. For any finite prime $p \notin S$, let $a_i(p)$ be the trace of $\rho_i(Frob_p)$. We say that the ρ_i are *λ-adically close near the supersingular primes* if there exists an integer $N_0 > 0$, such that for the primes p of K not in S and any integer $w > 0$,

$$\text{if both } a_i(p) \in \lambda^{N_0}, \text{ then } \lambda^w \mid a_1(p) \Leftrightarrow \lambda^w \mid a_2(p). \tag{1}$$

* Supported in part by NSF grant DMS 9304580 and by an NSERC postdoctoral fellowship.

0022-314X/99 $30.00

Given two such representations, we would like to know if they are the same up to the following operations:

- twist by a continuous character $G_K \to \mathcal{O}^\times$;
- conjugation by a matrix in $GL_n(\mathcal{O})$;
- the transpose-inverse automorphism of $GL_n(\mathcal{O})$; and
- a ring automorphism of $\mathcal{O}$.

Our main result is as follows.

THEOREM 1. *Let $\mathcal{O}$ be a commutative complete local ring with residue field k. Let $\rho_1, \rho_2: G_K \to GL_n(\mathcal{O})$ be surjective and be λ-adically close near the supersingular primes. Then they are the same up to the four operations above, provided that*

- *$\mathcal{O}$ is a domain and $k \neq \mathbb{F}_2, \mathbb{F}_3$; or*
- *$\mathcal{O}$ is Noetherian, $n \geqslant 4$ is even and $\mathrm{char}(k) > 2$; or $n = 2$ and $k \not\simeq \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5$; or*
- *$\mathcal{O}$ is Noetherian, n is odd, $k \not\simeq \mathbb{F}_2$, and, if $n = 3$, $k \not\simeq \mathbb{F}_3$.*

In the case $n = 3$ and $k \simeq \mathbb{F}_3$ or $n = 2$ and $\mathcal{O} = \mathbb{Z}/l^N$ with $l = 3$ or 5, the theorem holds for the pair of representations $G_K \to GL_n(\mathbb{Z}/l^{N-1})$ induced from the ρ_i.

COROLLARY 1. (a) *Let $\rho_1, \rho_2: G_K \to GL_2(\mathbb{Z}_l)$ be the l-adic representations associated to two elliptic curves E_1, E_2 defined over K. If the ρ_i are l-adically close near the supersingular primes, and either one of the E_i is CM or l is sufficiently large, then E_1 and E_2 are isogenous over $\bar{K}$.*

(b) *Let $\rho_1, \rho_2: G_K \to GL_2(\mathbb{Z}/l^n\mathbb{Z})$ be the G_K-action on the l^n-torsion points of the E_i. If the ρ_i are surjective and are l-adically close near the supersingular primes, and if $l > 5$, then the ρ_i differ by the twist of a character $G_K \to (\mathbb{Z}/l^n)^\times$.*

(c) *If $l = 3$ or 5, then conclusion for part* (b) *holds for the pair of representations $G_K \to GL_2(\mathbb{Z}/l^{n-1})$ induced from the ρ_i.*

Suppose $\mathcal{O}$ is either an integral domain, or $k \not\simeq \mathbb{F}_2$ and, if $n = 3$, $k \not\simeq \mathbb{F}_3$. The Goursat lemma reduces Theorem 1 to determining the automorphisms of $PGL_n(\mathcal{O})$ (Lemma 7). This second problem is a special case of the "automorphism problem of classical groups" and has a long history. The automorphisms of PGL_n over an integral domain, and those of GL_n over any ring and $n \geqslant 3$, have been determined; however, there are few results for $PGL_n(R)$ over non-integral domains such as $\mathbb{Z}/m$. In Section 2 we first summarize from the literature the known results on the automorphism

problem for linear groups, and then extend these results to determine $Aut(PGL_n(\mathcal{O}))$ and $Aut(GL_2(\mathcal{O}))$ for the rings $\mathcal{O}$ as above under mild conditions on $char(k)$ and n.

THEOREM 2. *Let R be a commutative local ring with residue field k. Let $l = char(k)$. Then the automorphisms of $PGL_n(R)$ are standard if one of the following statements holds*:

(a) *R is a domain and either $n \geqslant 3$, or $n = 2$ and $l \neq 2$;*

(b) *R is complete, $n \geqslant 3$ and $l \neq 2$, and, if $n = 4$, then R is Noetherian;*

(c) *R is Noetherian, $l \nmid n$, and*

- *$n = 2$ and $k \not\cong \mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_3$; or*
- *$n = 3$ and $l > 2$; or*
- *$n > 3$.*

In particular, Theorem 2 shows that every automorphism of $PGL_2(\mathbb{Z}/l^n)$ is standard if $l > 5$. On the other hand, McQuillan [14] showed that $PSL_2(\mathbb{Z}/l^n)$ has non-standard automorphisms if $l = 3$ or 5 and if $n > 1$. Building upon McQuillan's work we obtain the following result (cf. Section 2 for the definitions of standard automorphisms).

THEOREM 3. *Let $l = 3$ or 5, and let $\alpha \in (\mathbb{Z}/l^n)^\times$ be an element of order 2 or 4, respectively. Let $v, t \in \mathbb{Z}/l^n$ be divisible by l^{n-1}. Moreover, $t = 0$ or 3 if $l = 3$ and $n = 2$. Then there is an automorphism $\varphi_{v,t}$ of $PGL_2(\mathbb{Z}/l^n)$ given by*

$$\varphi_{v,t}\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ t & t+1 \end{pmatrix},$$

$$\varphi_{v,t}\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & t-1 \\ t+1 & 0 \end{pmatrix},$$

$$\varphi_{v,t}\begin{pmatrix} \alpha & 0 \\ 0 & t \end{pmatrix} = \begin{pmatrix} \alpha & v \\ v & 1 \end{pmatrix}.$$

Every automorphism of $PGL_2(\mathbb{Z}/l^n)$ is the compositum of a standard one with some $\varphi_{v,t}$.

Note that Theorem 2 does not cover the case where R is the completion of the ring of integers of a number field at a prime of residual characteristic 2. To handle these rings we employ a method of Landin and Reiner [8].

THEOREM 4. *Let R be a commutative PID with more than 4 units and $char(R) \neq 2$, such that $\mathbb{Z}[R^\times] = R$ or $(\mathbb{Z}/l)[R^\times] = R$ depending on whether*

char$(R)=0$ *or* $l>0$, *and that* $PSL_2(R)$ *is generated by the elements* $\left(\begin{smallmatrix}1 & r\\ 0 & 1\end{smallmatrix}\right)$ *with* $r\in R$ *and* $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$. *Then every automorphism of* $PGL_2(R)$ *is standard.*

Remark 1. Note that a complete local domain of characteristic $\neq 2$ satisfies the hypothesis of Theorem 4.

Remark 2. Corollary 1(b) is false for $l=2$; cf. Remark 5 and Lemma 9.

Remark 3. Under the hypothesis that $a_1(p)=\pm a_2(p)$ for almost all p, part (a) of the corollary was first proved by Serre [21, p. 324]. Note that Corollary 1(a) imposes condition only on a set of positive but arbitrarily small density.

By considering the symmetric square representations attached to the ρ_i, N. Katz and D. Ramakrishnan independently communicated to me a different argument of Corallary 1(a).

Remark 4. As Lang and Trotter [9, p. 6 ff] pointed out, the supersingular primes of an elliptic curve can be thought of as the elliptic curve analog of the primes that split completely in a Galois extension. Based on this heuristic, they asked if the supersingular primes alone determine the elliptic curve up to twist and isogeny. This question is in fact the original motivation of this paper. Corollary 1 gives a weak solution to this problem, by enlarging the set of primes in questions to an arbitrarily small "l-adic neighborhood of the supersingular primes."

If we try to study this question of Lang and Trotter by mimicking the proof of Theorem 1, we would need to verify the following

QUESTION. *Let* $\rho_1, \rho_2: G_{\mathbb{Q}}\to GL_1(\mathbb{Z}_l)$ *be the l-adic representations attached to two non-CM elliptic curve* E_1, E_2 *over* $\mathbb{Q}$. *Suppose that the* ρ_i *are surjective. Given* $\sigma\in G_{\mathbb{Q}}$ *such that* (*say*) $\rho_1(\sigma)$ *has trace zero, can we find a sequence of primes* $p_1, p_2, \ldots$ *which are supersingular for both* E_i, *such that the conjugacy classes* $\{Frob_{p_i}\}$ *converge to the class* $\{\sigma\}$ *in* $\mathbf{G}_{\mathbb{Q}}$?

This question presupposes the existence of infinitely many supersingular primes common to two elliptic curves. We do not have a single example of this phenomenon if the two curves are not related by isogeny and/or twist, but recent results of Fouvry and Murty [6] show that this is true on average. Note that given any elliptic curve E over $\mathbb{Q}$ and any integer $N>0$, the Chinese remainder theorem furnishes infinitely many curves over $\mathbb{Q}$, no two of which are $\bar{\mathbb{Q}}$-isomorphic to each other and to E, such that their $a(p)$'s are the same for the first N primes (including the bad primes).

Also, this question is open even when $E_1=E_2$. In fact, for $l>2$ there are two conjugacy classes of trace zero elements in $PGL_2(\mathbb{Z}_l)$, and we do not even know if each class contains one, let alone infinitely many, supersingular Frobenius of a fixed elliptic curve.

2. AUTOMORPHISMS OF GL_N AND PGL_N OVER LOCAL RINGS

Let φ be an automorphism of a commutative ring R; it induces an automorphism of $PGL_n(R)$. For any idempotent element $e \in R$ and any $g \in PGL_n(R)$, the map $x \mapsto g[\varphi(e(x^{-1t} + (1-e)\,x)]\,g^{-1}$ is called a *standard automorphism* of $PGL_n(R)$. Similarly, if γ: $GL_n(R) \to R^\times$ is a group homomorphism and $g \in GL_n(R)$, the map $x \mapsto \gamma(x) \cdot g[\varphi(e(x^{-1})^t + (1-e)x)]\,g^{-1}$ is called a *standard automorphism* of $GL_n(R)$. The *automorphism problem* of $PGL_n(R)$ and $GL_n(R)$ ask if the automorphisms of each of these groups are all standard.

This problem has a long history, going back to Schreier and van der Waerden [19] who studied PSL_n ($n \geqslant 3$) over a field. For general rings (even polynomial rings over a field when $n = 2$) there could be extra automorphisms, and the cases where 2 is not a unit in R or where $n \leqslant 3$ require special treatments; cf. [13, Section II.G] for a discussion of the history as well as the different approaches to the automorphism problem of classical groups; [7] and its bibliography for the recent developments; and [25] for the scheme-theoretic interpretation of the standard automorphisms.

Denote by $E_2(R)$ the subgroup of $SL_2(R)$ generated by the matrices $\left(\begin{smallmatrix} 1 & r \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ r & 1 \end{smallmatrix}\right)$. It coincides with $SL_2(R)$ if R is a Euclidean domain or a local ring [2]. We summarize the results in the literature on the automorphism problems of GL_n and PGL_n as follows:

THEOREM 5. *The automorphisms of $SL_n(R)$, $GL_n(R)$ and $PGL_n(R)$ are standard if R and n satisfy one of the following conditions* (*all rings are commutative*):

(a) *R is any integral domain and $n \geqslant 3$* (*cf.* [15] *for GL_n*, [22] *for PGL_n*);

(b) *R is any commutative ring and $n \geqslant 4$* [17]; *or 2 is a unit in R and $n \geqslant 3$* [25];

(c) *R is any integral domain such that $SL_2(R) = E_2(R)$*:

- *for $GL_2(R)$: $char(R) > 0$, or $char(R) = 0$ and 2 is a unit* [4];
- *for $PGL_2(R)$: 2 is a unit* [4];

(d) *for $SL_3(R)$: R is any semi-local ring* [12];

(e) *for $SL_2(R)$ and $GL_2(R)$ only*: *R is any local ring with residue field different from $\mathbb{F}_2$, $\mathbb{F}_3$ and $\mathbb{F}_5$* [24].

In addition to the cases above, the automorphisms of $GL_n(R)$ have been completely determined in the following cases:

(f) *R is arbitrary and $n = 3$* [10];

(g) *R is any commutative ring in which 2, 3 and 5 are units, and $n=2$* [11];

(h) *R is a local ring of characteristic 2 and $n=2$* [23].

THEOREM 6 (McQuillan [14]). *Let $l=3$ or 5, and let $n\geqslant 2$. Let t be an integer divisible by l^{n-1}, with $t=0$ or 3 if $l=3$ and $n=2$. Then there is an automorphism φ_t of $PSL_2(\mathbb{Z}/l^n\mathbb{Z})$ determined by the following*:

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}\mapsto\begin{pmatrix}1 & 1\\ t & 1+t\end{pmatrix},\qquad \begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\mapsto\begin{pmatrix}0 & t-1\\ t+1 & 0\end{pmatrix}. \tag{2}$$

Every automorphism of $PSL_2(\mathbb{Z}/l^n)$ is the composition of a standard one with some φ_t. In particular, the size of $Aut(PSL_2(\mathbb{Z}/l^n\mathbb{Z})$ is

$$\begin{cases}\#PGL_2(\mathbb{Z}/l^n\mathbb{Z})\times 2 & \text{if } n=2 \text{ and } l=3;\\ \#PGL_2(\mathbb{Z}/l^n\mathbb{Z})\times l & \text{if } n\geqslant 2 \text{ and } l=5, \quad \text{or if } n\geqslant 3 \text{ and } l=3.\end{cases}$$

In connection with our study of twists of Galois representations we need to determine $Aut(PGL_n(R))$, where R is a complete local ring and $n\geqslant 2$. Theorem 2(a) follows from the first three cases of Theorem 5. Theorem 2(b) follows from the classical method of involutions, a very elegant and conceptual approach which however requires $n\geqslant 3$ and 2 be a unit in R; cf. [13, p. 91 ff] for an exposition of the method for GL_n over a local ring, and [3, Section 7 and Section 9] for techniques to handle the projective case. In the rest of this section we employ a cohomological device to reduce Theorem 2(c) to determining the automorphisms of GL_n over the corresponding local rings.

For the rest of this section, let R be a Noetherian local ring with maximal ideal $\mathfrak{m}$ and residual field k. Let $l=char(k)$. For any object X defined over R, denote by $\bar{X}$ its reduction modulo $\mathfrak{m}$.

LEMMA 1. *If $l=0$ or $l\nmid n$, then l does not divide the cardinality of $R_n:=\{r\in R: r^n=1\}$.*

Proof. Since R is Noetherian and local, Krull's theorem [1, Thm. 10.17] implies that the natural map from R to its $\mathfrak{m}$-adic completion $R_{\mathfrak{m}}$ is injective. Since R_n is a subgroup of $\{x\in R_{\mathfrak{m}}: x^n=1\}$, it suffices to prove the lemma under the extra hypothesis that R is completed.

Since $l=0$ or $l\nmid n$, Hensel's lemma furnishes a bijection between R_n and the set $\{r\in k: r^n=1\}$, which is a subgroup of the group of nth roots of unity in k_a, the algebraic closure of k. The latter group has n elements, since $l=0$ or $l\nmid n$ implies that the roots of x^n-1 in k_a are distinct. Consequently, $l\nmid \#R_n$. ∎

Denote by $\mathscr{S}_n \subset SL_n(R)$ the subgroup of scalar matrices, so $\mathscr{S}_n \simeq R_n$. Denote by $\phi \in H^2(PSL_n(R), \mathscr{S}_n)$ the cohomology class corresponding to the extension

$$1 \to \mathscr{S}_n \to SL_n(R) \xrightarrow{\pi} PSL_n(R) \to 1. \tag{3}$$

Then an automorphism φ of $PSL_n(R)$ lifts to an automorphism of $SL_n(R)$ if and only if $(\varphi \circ \pi)^* \phi = 0$.

LEMMA 2. *Suppose that $l > 0$ and $l \nmid n$. Then the automorphisms of $PSL_n(R)$ lifts to those of $SL_n(R)$.*

Proof. K_n is the inverse limit of the finite l-groups $\ker(PSL_n(R/\mathfrak{m}^i) \to PSL_n(R/\mathfrak{m}))$, and hence it is a pro-$l$ group. Denote by PK_n the image of K_n in $PSL_n(R)$. Lemma 1 then implies that $H^i(K_n, \mathscr{S}_n)$ and $H^i(PK_n, \mathscr{S}_n)$ are trivial for $i > 0$. Dimension shifting plus the inflation-restriction sequence then gives the commutative diagram.

$$\begin{array}{ccc} H^2(PSL_n(R)/PK_n, \mathscr{S}_n^{PK_n}) & \xrightarrow{\sim} & H^2(PSL_n(R), \mathscr{S}_n) \\ \downarrow{\scriptstyle (\overline{\varphi \circ \pi})^*} & & \downarrow{\scriptstyle (\varphi \circ \pi)^*} \\ H^2(SL_n(R)/K_n, \mathscr{S}_n^{K_n}) & \xrightarrow{\sim} & H^2(SL_n(R), \mathscr{S}_n). \end{array} \tag{4}$$

Since (3) is a *central* extension, K_n and PK_n act trivially on $\mathscr{S}_n$. Moreover, since $l \nmid n$, as in the proof of Lemma 1 we can identify $\mathscr{S}_n$ with $\bar{\mathscr{S}}_n$. Thus the left column of (4) can be replaced by

$$H^2(PSL_n(k), \bar{\mathscr{S}}_n) \to H^2(SL_n(k), \bar{\mathscr{S}}_n).$$

In particular, the inverse image of ϕ under the top arrow of (4) corresponds to the reduction modulo $\mathfrak{m}$ of the extension (3), so $(\varphi \circ \pi)^* = 0$ precisely when $\overline{\varphi \circ \pi}$ can be lifted from $PSL_n(k)$ to $SL_n(k)$. Since the automorphisms of PSL_n over a field are standard, we are done. ∎

COROLLARY 2. *Let l, n and t be as in theorem* 6. *Then* (2) *defines an automorphism Φ_t of $SL_2(\mathbb{Z}/l^n)$, and every automorphism of $SL_2(\mathbb{Z}/l^n)$ is the composition of a standard one with some Φ_t.*

Proof. Let Φ_t be an automorphism of $SL_2(\mathbb{Z}/l^n)$, as furnished by Lemma 2, which lifts φ_t. Since $(\mathbb{Z}/l^n)^\times$ is cyclic, we have

$$\Phi_t \begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} = \varepsilon_1 \begin{pmatrix} 1 & 1 \\ t & t+1 \end{pmatrix} \quad \text{and} \quad \Phi_t \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \varepsilon_2 \begin{pmatrix} 0 & t-1 \\ t+1 & 0 \end{pmatrix}$$

with $\varepsilon_1, \varepsilon_2 \in \{\pm 1\}$. By [14, Prop. 4], $\Phi_t \pmod l$ is an automorphism of $SL_2(\mathbb{Z}/l)$, and hence it is given by conjugation by some matrix $A \in SL_2(\mathbb{Z}/l)$. In particular, $\Phi_t \pmod l$ preserves traces, whence $\varepsilon_1 = 1$ since $l > 2$. Thus A commutes with $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, whence $A = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)$ for some $a \pmod l$. Now, $\left(\begin{smallmatrix} -a & -a^2-1 \\ 1 & -a \end{smallmatrix}\right) = \left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)\left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)\left(\begin{smallmatrix} 1 & a \\ 0 & 1 \end{smallmatrix}\right)^{-1} \equiv \varepsilon_2 \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right) \pmod l$, whence $\varepsilon_2 = 1$. This proves the first part of the corollary. To prove the second part, first note that every automorphism Φ of $SL_2(\mathbb{Z}/l^n)$ fixes the kernel of the projection $SL_2(\mathbb{Z}/l^n) \to PSL_2(\mathbb{Z}/l^n)$, so it suffices to show that if Φ induces the trivial map on $PSL_2(\mathbb{Z}/l^n)$ then Φ is in fact trivial. This is indeed the case, by setting $t = 0$ in the argument above. ∎

We can now complete the proof of case (c) of Theorem 2. Let φ be an automorphism of $PGL_n(R)$. Now, $PSL_n(R)$ is the commutator subgroup of $PGL_n(R)$: for $n \geqslant 3$ this is [16, Prop. 2]; for $n = 2$ this follows from [2, Thm. 4.1 and Prop. 9.2]. Thus φ must takes $PSL_n(R)$ to itself. Combine Theorem 5 with Lemma 2, we see that $\varphi|_{PSL_n(R)}$ is standard, so we can assume without loss of generality that $\varphi|_{PSL_n(R)}$ is trivial. Since $PGL_n(R)$ is generated by $PSL_n(R)$ and the diagonal matrices, we are reduced to study the φ-action on the latter ones.

Denote by $t_{ij}(x)$ the element in $PGL_n(R)$ represented by the matrix obtained by taking the identity matrix and replacing the ij-entry by x. Denote by $C_{ij}(x)$ the centralizer of $t_{ij}(x)$ in $PGL_n(R)$. Then for any $l > 0$ and $y \in R^\times$, $t_{ll}(y) \in \bigcap_{i,\, j,\, j \neq l} C_{ij}(1)$. This intersection consists of the diagonal matrices. Since φ fixes the $t_{ij}(x)$ if $i \neq j$, it follows that $\varphi(t_{ll}(y))$ is diagonal. For any $l > 1$, the commutator of $t_{mm}(y)$ and $t_{l,\, l-1}(-1)$ is $t_{l,\, l-1}(1-y)$ if $m = l$, and is trivial otherwise. It follows that φ fixes $t_{ll}(y)$. This completes the proof of case (c) of Theorem 2.

3. $PGL_2(\mathbb{Z}/l^N)$ FOR $l = 3$ AND 5

LEMMA 3. *Let R be a local ring whose residue field is not $\mathbb{F}_2$. Let φ be an automorphism of $PGL_2(R)$. Then φ takes $PSL_2(R)$ to itself. Moreover, if the restriction of φ to $PSL_2(R)$ is the identity map, then φ is the identity map.*

Proof. For a local ring R as above, the commutator subgroup of $GL_2(R)$ is $SL_2(R)$ [2; Thm. 4.1 and Prop. 9.2], whence the commutator subgroup of $PGL_2(R)$ is $PSL_2(R)$. The first part of the lemma then follows.

Let φ be as in the second part of the lemma. Pick an element $\mu \in R^\times$, and let $\left(\begin{smallmatrix} x & y \\ z & w \end{smallmatrix}\right) \in GL_2(R)$ be a lift of $\varphi\left(\begin{smallmatrix} 1 & 0 \\ 0 & \mu \end{smallmatrix}\right)$. We have the following identities in $GL_2(R)$:

$$\begin{pmatrix}1 & 0\\ 0 & \mu\end{pmatrix}\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \mu\end{pmatrix}^{-1}=\begin{pmatrix}1 & \lambda/\mu\\ 0 & 1\end{pmatrix},$$

$$\begin{pmatrix}1 & 0\\ 0 & \mu\end{pmatrix}\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix}\begin{pmatrix}1 & 0\\ 0 & \mu\end{pmatrix}^{-1}=\begin{pmatrix}1 & 0\\ \lambda\mu & 1\end{pmatrix}.$$

Since $\varphi|_{PSL_2(R)}$ is the identity, apply φ to both sides of the two identities above and we get, for some $\varepsilon_1, \varepsilon_2 \in R^\times$, the following identities in $GL_2(R)$:

$$\begin{pmatrix}x & y\\ z & w\end{pmatrix}\begin{pmatrix}1 & \lambda\\ 0 & 1\end{pmatrix}\begin{pmatrix}x & y\\ z & w\end{pmatrix}^{-1}=\varepsilon_1\begin{pmatrix}1 & \lambda/\mu\\ 0 & 1\end{pmatrix},$$

$$\begin{pmatrix}x & y\\ z & w\end{pmatrix}\begin{pmatrix}1 & 0\\ \lambda & 1\end{pmatrix}\begin{pmatrix}x & y\\ z & w\end{pmatrix}^{-1}=\varepsilon_2\begin{pmatrix}1 & 0\\ \lambda\mu & 1\end{pmatrix}.$$

Compare the entries and we get $y=z=0$, $\varepsilon_1=\varepsilon_2=1$, and $\mu=w/x$. Thus $\varphi\left(\begin{smallmatrix}1 & 0\\ 0 & \mu\end{smallmatrix}\right)=\left(\begin{smallmatrix}1 & 0\\ 0 & \mu\end{smallmatrix}\right)$ (in $PGL_2(R)$) for every $\mu \in R^\times$, whence φ is trivial. ∎

Proof of Theorem 3. For the rest of this section let $l=3$ or 5.

Let $\alpha \in (\mathbb{Z}/l^n)^\times$ be an element of order 2 (resp. 4) if $l=3$ (resp. $l=5$). Then $PGL_2(\mathbb{Z}/l^n)$ is generated by $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$, $\left(\begin{smallmatrix}0 & -1\\ 1 & 0\end{smallmatrix}\right)$, and $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$, and the group structure of $PGL_2(\mathbb{Z}/l^n)$ is determined by that of $PSL_2(\mathbb{Z}/l^n)$ along with the following relations: for every $x \in \mathbb{Z}/l^n$,

$$\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}=\begin{pmatrix}1 & \alpha x\\ 0 & 1\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}, \tag{5}$$

$$\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}^{-1}. \tag{6}$$

Let φ_t be an automorphism of $PSL_2(\mathbb{Z}/l^n)$ furnished by Theorem 6. To extend φ_t to $PGL_2(\mathbb{Z}/l^n)$ it then suffices to assign $\varphi\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$ and then show that φ preserves these two relations.

By [14, Prop. 2], $\varphi_t \pmod{l^{n-1}}$ is the identity automorphism of $PSL_2(\mathbb{Z}/l^{n-1})$. In view of Lemma 3, any extension φ of φ_t to $PGL_2(\mathbb{Z}/l^n)$ must be trivial mod l^{n-1}. Write $\varphi\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)=\left(\begin{smallmatrix}\alpha+u & v\\ w & 1+z\end{smallmatrix}\right)$ with $u, v, w, z \equiv 0 \pmod{l^{n-1}}$. Since φ must preserve (6), we get $v=w$, and from $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)^2=1$ if $l=3$ (resp. $\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)^4=1$ if $l=5$) we get

$$\varphi\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}=\begin{pmatrix}\alpha & v\\ v & 1\end{pmatrix}. \tag{7}$$

Since l^{n-1} divides t, for any integer m, we have (in $PGL_2(\mathbb{Z}/l^n)$)

$$\begin{aligned}\begin{pmatrix}1 & 1\\ t & 1+t\end{pmatrix}^m &= \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^m + t\sum_{j=0}^{m-1}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^j\begin{pmatrix}0 & 0\\ 1 & 1\end{pmatrix}\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}^{m-1-j}\\ &= \begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix} + t\sum_{k=1}^{m}\begin{pmatrix}m-k & (m-k)\,k\\ 1 & k\end{pmatrix}\\ &= \begin{pmatrix}1 & m\\ 0 & 1\end{pmatrix} + t\begin{pmatrix}m(m-1)/2 & (m^2-1)\,m/6\\ m & (m+1)\,m/2\end{pmatrix}.\end{aligned}$$

A straight-forward computation then shows that the relation (5) is preserved for any choice of $\varphi\left(\begin{smallmatrix}\alpha & 0\\ 0 & 1\end{smallmatrix}\right)$ in (7). This completes the proof of Theorem 3. ∎

4. PGL_2 OVER PID

Let R be a PID with more than 4 units and $char(R)\neq 2$, such that

$$\mathbb{Z}[R^\times] = R \qquad \text{or} \qquad (\mathbb{Z}/l)[R^\times] = R \tag{8}$$

depending on whether $char(R)=0$ or $char(R)=l>0$. Denote by K the quotient field of R, and by R^+ the additive group R. Define the following elements of $PGL_2(R)$:

$$I=\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, \qquad S=\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$$

$$[\alpha, 1]=\begin{pmatrix}\alpha & 0\\ 0 & 1\end{pmatrix}, \qquad X(\gamma)=\begin{pmatrix}1 & \gamma\\ 0 & 1\end{pmatrix},$$

where $\alpha\in R^\times$ and $\gamma\in R$. Note that the parameter in each of the projective matrices $[\alpha, 1]$ and $X(\gamma)$ is well-defined.

Conjugation by the element $M\in PGL_2(R)$ refers to map $A\mapsto MAM^{-1}$. Note that the transpose-inverse automorphism is the same as conjugation by S.

Now, suppose that $PSL_2(R)$ is generated by S and by the $X(\gamma)$'s; this is true for example if R is local [2, Thm. 4.1]. To determine the automorphisms of $PGL_2(R)$, it then suffices to determine their actions on S, the $[\alpha, 1]$'s, and the $X(\gamma)$'s. We do this in three steps, following closely the argument in [8].

An element $u\in PGL_2(R)$ is called a *transvection* if: in the case $char(R)=0$, there exists more than two elements in $PGL_2(R)$ which are $PGL_2(R)$-conjugate to and commute with u; in the case $char(R)=l>0$, we have $u\neq I$ and $u^l=I$ (this is *not* the standard definition).

LEMMA 4. *An element $u \in PGL_2(R)$ is a transvection if and only if it is conjugate in $PGL_2(R)$ to $X(\gamma)$ for some $\gamma \in R$, or, if $char(R) > 0$, to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.*

Proof. First, suppose $char(R) = 0$. Suppose that a lift to $GL_2(R)$ of the transvection u has distinct eigenvalues (this is independent of the choice of lifts). Then u is conjugate to $[\alpha, 1]$ (in PGL_2) for some $\alpha \neq 1$ in a field extension of K. If $w = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in GL_2(R)$ commutes with u up to scalar, then in a field extension of K, we have the following equality in $GL_2(R)$:

$$\begin{aligned}\begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix} &= wuw^{-1}u^{-1} \\ &= \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} \alpha & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} d & -b \\ -c & a \end{pmatrix}\begin{pmatrix} 1/\alpha & 0 \\ 0 & 1 \end{pmatrix}\frac{1}{ad-bc} \\ &= \begin{pmatrix} ad-bc/\alpha & ab(A-\alpha) \\ cd(1-1/\alpha) & ad-bc\alpha \end{pmatrix}\frac{1}{ad-bc}.\end{aligned}$$

Now, $\alpha \neq 1$ forces $ab = 0 = cd$, whence $w = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$ or $w = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$. Suppose that, in addition, w is $PGL_2(R)$-conjugate to u, so the eigenvalues of w are multiplies of those of u. If $w = \left(\begin{smallmatrix} a & 0 \\ 0 & d \end{smallmatrix}\right)$, then as projective matrices there are only two choices for w, contradicting the hypothesis. If $w = \left(\begin{smallmatrix} 0 & b \\ c & 0 \end{smallmatrix}\right)$, then $wuw^{-1}u^{-1} = \left(\begin{smallmatrix} 1/\alpha & 0 \\ 0 & \alpha \end{smallmatrix}\right)$ is a scalar, whence $\alpha = -1$ (since $\alpha \neq 1$). Consequently, u and w are PGL_2-conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$.

To recapitulate, either u is $PGL_2(R)$-conjugate to $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$, or u has repeated eigenvalues. In the second case, since R is a PID, u is $PGL_2(R)$-conjugate to $X(\gamma)$ for some $\gamma \in R$.

For the converse, note that $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ is $PGL_2(R)$-conjugate to $\left(\begin{smallmatrix} 0 & b \\ -1/b & 0 \end{smallmatrix}\right)$ for any $b \in R^\times$. So if R has more than 4 units, then there are more than two such matrices in $PGL_2(R)$. As for $X(\gamma)$, note that

$$[\beta, 1]\, X(\gamma)[\beta, 1]^{-1} = X(\beta\gamma)$$

commutes with and is conjugate to $X(\gamma)$. Just pick three different $\beta \in R^\times$ and we are done.

Finally, suppose $char(R) = l > 0$; then $X(\gamma)^l = I$ for all $\gamma \in R$. On the other hand, a transvection $u \in PGL_2(R)$ now satisfies the equation $u^l - I = (u - I)^l = 0$. Thus it has repeated eigenvalues, and hence it is $PGL_2(R)$-conjugate to $X(\gamma)$ for some $\gamma \in R$. ∎

Let φ be an automorphism of $PGL_2(R)$, and fix an element $\gamma_0 \in R$ such that $X(\gamma_0)^2 \neq 1$ in $PGL_2(R)$ (recall that R is a domain with $char(R) \neq 2$). Lemma 4 then implies that, composing φ with an inner automorphism if necessary, we have

$$\varphi(X(\gamma_0)) = X(\sigma(\gamma_0))$$

for a *unique* $\sigma(\gamma_0) \in R$. Since $X(\gamma)$ is a transvection and commutes with $X(\gamma_0)$, Lemma 4 implies that $\varphi(X(\gamma))$ is a transvection and commutes with $X(\sigma(\gamma_0))$. Thus for every $\gamma \in R$,

$$\varphi(X(\gamma)) = X(\sigma(\gamma)) \tag{9}$$

for a *unique* $\sigma(\gamma) \in R$. Moreover, as $X(s+t) = X(s)\,X(t)$, we see that σ is an automorphism of R^+.

LEMMA 5. *Let φ be an automorphism of $PGL_2(R)$. Compose φ with an inner automorphism if necessary, we can assume that* (9) *holds with $\sigma(1) = 1$ and $\varphi(S) = S$.*

Proof. First, adjust φ as above to get (9). We now study the φ-action on S. Let $Y = SX(1)$. We claim that $trace(\varphi(Y))$ is a unit (this statement is independent of the choice of lifts to $GL_2(R)$).

Since $Y^3 = I$, we see that $\varphi(Y)^3$ is a scalar, whence the minimal and the characteristic polynomials of any lift $\varphi(Y)$ coincide and divide $x^3 - r$ for some unit r. Thus $x^3 - r$ is reducible over R, and hence $r = \rho^3$ for some $\rho \in R^\times$.

If $char(R) = 3$, then $x^3 - r = (x-\rho)^3$, whence the characteristic polynomial of any lift of $\varphi(Y)$ is $(x-\rho)^2 = x^2 - 2\rho x + \rho^2$. Thus the trace of $\varphi(Y)$ is $-\rho \in R^\times$.

Now, suppose $char(R) \neq 3$. If $(x^3 - r)/(x-\rho) = x^2 + \rho x + \rho^2$ is irreducible over R, then the trace of $\varphi(Y)$ is $-\rho \in R^\times$. If it is reducible, so R contains a primitive third-root of unity ω, then the characteristic polynomial of $\tau(Y)$ is one of the following:

$$(x-\rho)(x-\omega\rho), \qquad (x-\rho)(x-\omega^2\rho), \qquad \text{or} \quad (x-\omega\rho)(x-\omega^2\rho).$$

The trace of $\varphi(Y)$ is then $-\omega^2\rho$, $-\omega\rho$ and $-\rho$, respectively; all these of these elements are units. Thus $trace(\varphi(Y)) \in R^\times$ in all cases.

Let $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ be a lift of $\varphi(S)$. Since $S^2 = -I$ is trivial in $PGL_2(R)$,

$$\varphi(S)^2 = \begin{pmatrix} a^2+bc & b(a+d) \\ c(a+d) & d^2+bc \end{pmatrix}$$

is a scalar, whence $a^2 + bc = d^2 + bc \in R^\times$ and $b(a+d) = c(a+d) = 0$. If $a + d \neq 0$, then $b = c = 0$, $a^2 = d^2 \in R^\times$, and $a \neq -d$, whence $\varphi(S)$ is a scalar, a contradiction. Thus $\varphi(S) = \left(\begin{smallmatrix} a & b \\ c & -a \end{smallmatrix}\right)$, and hence

$$\varphi(Y) = \varphi(S)\,\varphi(X(1)) = \begin{pmatrix} a & a\sigma(1)+b \\ c & c\sigma(1)-a \end{pmatrix}.$$

As $trace(\varphi(Y)) = c\sigma(1)$ is a unit, so is c. Let φ_1 be the composition of φ with conjugation by $X(-a/c)$; then

$$\varphi(S) = \begin{pmatrix} 0 & b + a^2/c \\ c & 0 \end{pmatrix}.$$

On the other hand, since $Y^3 = I$,

$$\varphi(Y)^3 = \begin{pmatrix} * & * \\ c^3\sigma(1) + c^2 b + ca^2 & * \end{pmatrix}$$

is a scalar. Thus $c^2\sigma(1) + cb + a^2 = 0$, whence

$$\varphi_1(S) = \begin{pmatrix} 0 & -c\sigma(1)^2 \\ c & 0 \end{pmatrix} = \begin{pmatrix} 0 & \sigma(1)^2 \\ -1 & 0 \end{pmatrix}$$

in $PGL_2(R)$. In particular, $\sigma(1) \in R^\times$. Finally, let φ_2 be the composition of φ_1 with conjugation by $[1/\sigma(1), 1]$, then (9) is preserved and with $\sigma(1) = 1$, while $\varphi_2(S) = S$ in $PGL_2(R)$, as desired. ▮

LEMMA 6. *Let φ be an automorphism of $PGL_2(R)$ as furnished by Lemma 5. Then σ is a ring automorphism of R, and $\varphi([\alpha, 1]) = [\sigma(\alpha), 1]$.*

Proof. Let $G \subset PGL_2(R)$ be the subgroup generated by the $X(\gamma)$'s. Then φ takes G as well as its transpose to itself (the latter follows from $X(\gamma)^t = SX(-\gamma)S^{-1}$), and hence it stabilizes the intersection of the normalizer of each of G and G^t. This intersection consists of precisely the diagonal matrices in $PGL_2(R)$, so $\varphi([\alpha, 1]) = [\rho(\alpha), 1]$ for some endomorphism ρ of $R^\times$. Apply φ to both sides of $X(\alpha\gamma) = [\alpha, 1]\, X(\gamma)[\alpha, 1]^{-1}$ then gives $\sigma(\alpha\gamma) = \rho(\alpha)\,\sigma(\gamma)$. As $\sigma(1) = 1$, we see that for $\alpha \in R^\times$ and $\gamma \in R$,

$$\rho(\alpha) = \sigma(\alpha), \qquad \sigma(\alpha\gamma) = \sigma(\alpha)\,\sigma(\gamma). \tag{10}$$

From $\sigma(1) = 1$ and the additivity of σ we get $\sigma(a) = a$ for every $a \in \mathbb{Z}$ (resp. $\mathbb{Z}/l$, if $char(R) = l > 0$). Condition (8) plus (10) then implies that σ is R-multiplicative. As σ is bijective on $R^\times$, we are done. ▮

Combining everything then gives Theorem 4.

5. TWISTS OF GALOIS REPRESENTATIONS

We now come to the proof of Theorem 1. We follow the notation in the introduction. Denote by $\tilde{\rho}_i$ the projective representation $G_K \to PGL_n(\mathcal{O})$ induced from ρ_i.

LEMMA 7. *Let $\mathcal{O}$ be a commutative, complete local ring with maximal ideal λ. Let $\rho_1, \rho_2: G_K \to GL_n(\mathcal{O})$ be surjective and λ-adically close near the supersingular primes. Suppose that one of the followings holds*:

- *$\mathcal{O}$ is an integral domain and $k \neq \mathbb{F}_2, \mathbb{F}_3$; or*
- *n is even and $k \not\simeq \mathbb{F}_2$; or*
- *n is odd, $k \not\simeq \mathbb{F}_2$, and, in addition, $k \not\simeq \mathbb{F}_3$ if $n = 3$,*

then there exists an automorphism φ of $PGL_n(\mathcal{O})$ such that $\varphi \circ \tilde{\rho}_2 = \tilde{\rho}_1$.

Suppose $\mathcal{O}$ is not an integral domain, with n even and $k \simeq \mathbb{F}_2$, or with $n = 3$ and $k \simeq \mathbb{F}_3$. Denote by N the largest integer such that $\lambda^N \neq 0$ in $\mathcal{O}$. Then the same conclusion holds for the pairs of representations $G_K \to GL_n(\mathcal{O}/\lambda^N)$ induced from the ρ_i.

Proof. Let $G_1, G_2 = PGL_n(\mathcal{O})$. Let H be the image of $\tilde{\rho} = (\tilde{\rho}_1, \tilde{\rho}_2)$: $G_K \to G_1 \times G_2$. Denote by $\pi_i = H \to G_i$ the projection of H to G_i. The image of H in $G_1/\pi_1(\ker \pi_2) \times G_2/\pi_2(\ker \pi_1)$, by Goursat's lemma [18; Lemma 3.2.], is the graph of an isomorphism, so we are reduced to show that both π_i are injective. We divide the argument into two cases depending on the parity of n. Denote by J_n the $n \times n$ matrix whose ij-entry is 1 if $i + j = n + 1$, and is zero otherwise.

One important remark before we continue: while the trace of an element of $PGL_n(\mathcal{O})$ is well-defined only up to a unit, since $\mathcal{O}$ is complete it makes perfect sense to say that an element of $PGL_n(\mathcal{O})$ has trace zero, namely its trace is 0 (mod λ^w) for every $w > 0$.

Continue with the proof, suppose first that n is even and $k \not\simeq \mathbb{F}_2$, whence there exists $a \in \mathcal{O}^\times$ such that $1 - a \in \mathcal{O}^\times$. Pick any integer $\mu \in \{1, ..., n\}$. Since ρ_2 is surjective, we can find $\sigma_1, \sigma_2, \sigma_3 \in G_K$ such that the matrix $\rho_2(\sigma_k)$ is obtained from J_n by replacing the 2×2 minor at (μ, μ), $(\mu, n-\mu)$, $(n-\mu, \mu)$ and $(n-\mu, n-\mu)$ by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$, $\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$, and $\left(\begin{smallmatrix} 0 & 1 \\ a & 0 \end{smallmatrix}\right)$, respectively. Fix an element $\tilde{\rho}(\sigma) = (I_n, M) \in \ker \pi_1$, and write $\pi_2(\tilde{\rho}(\sigma)) = (m_{ij})_{i,j}$.

Since the Frobenius conjugacy classes are dense in G_K, we can pick a sequence of primes $\{p_i\}_i$ whose Frobenius classes converge in G_K to the class of σ_k. For any fixed $w > 0$, the continuity of ρ_2 implies that for i sufficiently large (with respect to w),

$$0 = trace(\rho_2(\sigma_k)) \equiv trace(\rho_2(Frob_{p_i})) \qquad (\text{mod } \lambda^w).$$

If w is sufficiently large, condition (1) implies that

$$trace(\rho_1(Frob_{p_i})) \equiv 0 \qquad (\text{mod } \lambda^w).$$

By the continuity of ρ_1, we get

$$trace(\rho_1(\sigma_k)) \equiv 0 \qquad (\text{mod } \lambda^w).$$

Since this holds for every w and $\mathcal{O}$ is complete, $trace(\rho_1(\sigma_k)) = 0$. By our earlier remark on projective traces, we can write

$$\begin{aligned} 0 = trace(\tilde{\rho}_1(\sigma_k)) &= trace(\pi_1(\tilde{\rho}(\sigma_k))) \\ &= trace(\pi_1(\tilde{\rho}(\sigma_k)\cdot\tilde{\rho}(\sigma))) \\ &= trace(\pi_1(\tilde{\rho}(\sigma_k\sigma))). \end{aligned}$$

Apply the continuity argument as before, we get

$$\begin{aligned} 0 &= trace(\pi_2(\tilde{\rho}(\sigma_k\sigma))) \\ &= trace(\tilde{\rho}_2(\sigma_k)\cdot m) \\ &= \sum_{i\neq \mu, n-\mu}^{n} m_{i,n-i} + \begin{cases} m_{\mu,\mu} - m_{n-\mu,n-\mu} & k=1; \\ m_{\mu,n} + m_{n-\mu,\mu} & k=2; \\ am_{\mu,n-\mu} + m_{n-\mu,\mu} & k=3. \end{cases} \end{aligned}$$

As μ runs through all integers between 1 and n, we get $m_{ii} = m_{jj}$ for all i, j and $(1-a)\,m_{ij} = 0$ if $i \neq j$. Since $1-a \in \mathcal{O}^\times$, it follows that $\pi_2(\tilde{\rho}(\sigma))$ is a scalar matrix. But $\pi_2(\tilde{\rho}(\sigma)) \in PGL_n(\mathcal{O})$, so $\tilde{\rho}(\sigma)$, and hence $\ker \pi_1$ is trivial. The same holds for $\ker \pi_2$, by symmetry.

If n is even and $k \simeq \mathbb{F}_2$, then repeat the argument above with $a = -1$ and we see that $2\pi_2(\tilde{\rho}(\sigma))$ is a scalar matrix, and the theorem follows in this case.

Next, suppose that $n \geqslant 3$ is odd. Pick two distinct integers μ, ν between 1 and n. Since ρ_2 is surjective, we can find $\sigma_1, ..., \sigma_{14}$ such that for $k = 1, ..., 14$, the matrix $\rho_2(\sigma_k)$ is obtained from J_n by replacing the 3×3 minor whose coordinates involve one of μ, ν, $n-\mu$, by

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & -a-1 \end{pmatrix}, \quad \begin{pmatrix} a & 0 & 0 \\ 0 & -a-1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -a-1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & a \end{pmatrix};$$

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & -a-1 & 0 \\ 0 & 0 & a \end{pmatrix}, \quad \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -a-1 \end{pmatrix}, \quad \begin{pmatrix} -a-1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & 1 \end{pmatrix};$$

$$\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & b^{\varepsilon_2} \\ b^{\varepsilon_1} & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & b^{\varepsilon_2} \\ 1 & 0 & 0 \\ 0 & b^{\varepsilon_1} & 0 \end{pmatrix},$$

where $a \in R^\times$ is chosen so that $a+1 \in R^\times$; $b \in R^\times$ is chosen so that $1-b \in R^\times$; and $\varepsilon_1 \in \{0, 1\}$. Pick $m = (I_n, M) \in \ker \pi_1$, and write $M = (m_{ij})_{i,j}$. As we run through all σ_k, we get as before a system of equations

$$\begin{cases} am_{\mu,\mu} - (a+1)\, m_{\nu,\nu} + m_{n-\mu,n-\mu} = 0, \\ m_{\mu,\mu} + am_{\nu,\nu} - (a+1)\, m_{n-\mu,n-\mu} = 0, \end{cases}$$

$$\begin{cases} m_{\mu,\mu} + am_{\nu,\nu} - (a+1)\, m_{n-\mu,n-\mu} = 0, \\ (-a-1)\, m_{\mu,\mu} + am_{\nu,\nu} + m_{n-\mu,n-\mu} = 0, \end{cases}$$

$$\begin{cases} m_{\nu,\mu} + b^{\varepsilon_1} m_{n-\mu,\nu} + b^{\varepsilon_2} m_{\mu,n-\mu} = 0, \\ b^{\varepsilon_2} m_{n-\mu,\mu} + m_{\mu,\nu} + b^{\varepsilon_1} m_{\nu,n-\mu} = 0, \end{cases}$$

from which we get

$$\begin{aligned} (a^2+a+1)\, m_{\nu,\nu} &= (a^2+a+1)\, m_{n-\mu,n-\mu}, \\ (a+2)\, m_{\mu,\mu} &= (a+2)\, m_{n-\mu,n-\mu}, \\ 0 &= (1-b)\, m_{\mu,\nu}, \qquad \text{if} \quad \mu \neq \nu. \end{aligned}$$

If $k \not\simeq \mathbb{F}_2$ or $\mathbb{F}_3$, there exists $a \in R^\times$ so that $a+1 \in R^\times$, and that one of a^2+a+1 or $a+2$ is in $R^\times$. Thus $\ker \pi_1 = 0$ for such k. If $k \simeq \mathbb{F}_3$, then we can only assert that the off-diagonal entries of M are all zero, and that 3 times the diagonal entries are equal, whence $3 \ker \pi_1 = 0$. Finally, suppose $n \geqslant 5$. Repeat the calculation above using cyclic permutations of the 5×5 diagonal matrix with diagonal entries 1, 1, 1, 1, -4, we get, for distinct 5-tuple of indices $(\alpha, \beta, \gamma, \delta, \varepsilon)$, the relation $m_{\alpha,\alpha} + m_{\beta,\beta} + m_{\gamma,\gamma} + m_{\delta,\delta} - 4m_{\varepsilon,\varepsilon} = 0$ and cyclic permutations of these. Combine these with the above, we get $5 \ker \pi_1 = 0$, whence $\ker \pi_1 = 0$. ∎

In view of lemma 7, we can adjust ρ_2 by a standard automorphism of $GL_n(\mathcal{O})$ so that $\tilde{\rho}_1 = \tilde{\rho}_2$. Then ρ_1, ρ_2 are lifts to $GL_2(\mathcal{O})$ of the same projective representation. Theorem 1 now follows from the following elementary fact.

LEMMA 8. *Let $1 \to C \to \tilde{H} \to H \to 1$ be a central extension of groups. Then any two lifts to $\tilde{H}$ of a map $G \to \tilde{H}$ differ by the twist of a map $G \to C$.* ∎

For GL_2, the transpose-inverse automorphism is he same as conjugation by $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$; moreover, $\mathbb{Z}_l$ has no non-trivial ring automorphisms. Thus the standard automorphisms of $GL_2(\mathbb{Z}_l)$ are simply the conjugations, and Corollary 1 follows.

Remark 5. Theorem 1 does not handle non-integral domains $\mathcal{O}$ with $char(k) = 2$, partly due to our incomplete knowledge of $Aut(PGL_n(\mathcal{O}))$ in

that case. For $n \geqslant 3$, it would be interesting to see if the techniques of [10, 17] are applicable. Note that since $GL_n(\mathbb{F}_2) \simeq PSL_n(\mathbb{F}_2)$ is simple if $n \geqslant 3$, our argument shows that Theorem 1 is true if $n \geqslant 3$ and $\mathcal{O} \simeq \mathbb{F}_2$.

For $n = 2$, the theorem as is stated is false for rings $\mathcal{O}$ with $char(k) = 2$; the lemma below will provide plenty of counterexamples. Given that, it might not be unreasonable to expect that, say in the case $\mathcal{O} \simeq \mathbb{Z}/2^n$, the situation will stabilize for $n \geqslant 3$ (cf. [20, p. IV-28]).

LEMMA 9. *Let $\rho_1, \rho_2 : G_K \to GL_2(\mathbb{Z}/2\mathbb{Z})$ be continuous, surjective Galois representations. Denote by K_i the splitting field of ρ_i over K. Then the condition*

$$\text{for almost all } p, \qquad a_1(p) \equiv a_2(p) \pmod 2$$

is equivalent to $K_1 \cap K_2$ containing the unique quadratic subfield of both K_i/K.

Proof. Since $\mathrm{Gal}(K_i/K) \simeq GL_2(\mathbb{Z}/2\mathbb{Z}) \simeq S_3$, for an unramified prime p we have $a_i(p) \equiv 0 \pmod 2$ if and only if $\rho_i(Frob_p)$ has order 1 or 3; that in turn is true if and only if p splits in the unique quadratic subfield of K_i/K. The lemma then follows. ∎

ACKNOWLEDGMENTS

I thank F. Hajir, K. Murty, K. Rubin, and C. Skinner for useful discussions. I am indebted to J. Hoffstein for bringing to my attention the question about twists an the $a(p)$'s, K. Ribet for bringing my attention to Serre's work, N. Katz and D. Ramakrishnan for showing me the symmetric square argument, D. Rohrlich for his careful reading of an earlier version of the manuscript, and the referee for his comments.

This paper was written during my stay at the Institute for Advanced Study. I thank the Institute for their hospitality and support.

REFERENCES

1. M. F. Atiyah and I. G. Macdonald, "Introduction to Commutative Algebra," Addison–Wesley, Reading, MA, 1969.
2. P. M. Cohn, On the structure of the GL_2 of a ring, *Inst. Hautes Etudes Sci. Publ. Math.* **30** (1966), 5–54.
3. J. Dieudonné, On the automorphisms of the classical groups, *Mem. Amer. Math. Soc.* **2** (1951),.
4. M. H. Dull, Automorphisms of the two-dimensional linear groups over integral domains, *Amer. J. Math.* **96** (1974), 1–40.
5. N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over **Q**, *Invent. Math.* **89**(3) (1987), 561–567.
6. E. Fouvry and R. Murty, Supersingular primes common to two elliptic curves, *in* "Number Theory, (Paris, 1992–1993)," London Math. Soc. Lecture Note Ser., Vol. 215, pp. 91–102, Cambridge Univ. Press, Cambridge, UK, 1995.

7. A. Hahn and O. T. O'Meara, "The Classical Groups and K-Theory," Springer-Verlag, Berlin/New York, 1989.
8. J. Landin and I. Reiner, Automorphisms of the two-dimensional general linear groups over a Euclidean ring, *Proc. Amer. Math. Soc.* **9** (1958), 209–216.
9. S. Lang and H. Trotter, "Frobenius Distributions in GL_2-Extensions," Lecture Notes in Math., Vol. 504, Springer-Verlag, Berlin/New York, 1976.
10. F. Li and Z. Li, Isomorphisms of GL_3 over commutative rings, *Sci. Sinica Ser. A* **31**(1) (1988), 7–14.
11. F. Li and H. S. Ren, The automorphisms of two-dimensional linear groups over commutative rings, *Chinese Ann. Math. Ser. B* **10**(1) (1989), 50–57.
12. B. R. McDonald, Automorphisms of $GL_n(R)$, *Trans. Amer. Math. Soc.* **215** (1976), 145–159.
13. B. R. McDonald, "Geometric Algebra over Local Rings," Dekker, New York, 1976.
14. D. L. McQuillan, Some results on the linear fractional group III, *J. Math* **10** (1966), 24–38.
15. O. T. O'Meara, The automorphisms of the linear groups over any integral domain, *J. Reine Angew. Math.* **233** (1966), 56–100.
16. V. M. Petechuk, Automorphisms of the groups SL_n and GL_n over certain local rings, *Mat. Zametki* **28**(2) (1980), 187–204, 318.
17. V. M. Petechuk, Automorphisms of matrix groups over commutative rings., *Mat. Sb* **117** (159) (4) (1982), 534–547, 560.
18. K. Ribet, On l-adic representations attached to modular forms, *Invent. Math.* **28** (1975), 245–275.
19. O. Schreier and B. L. van der Waerden, Die automorphismem der projektiven Gruppen, *Abh. Math. Sem. Univ. Hamburg* **6** (1928), 303–332.
20. J. P. Serre, "Abelian l-adic Representations and Ellipic Curves," Benjamin, Elsmford, NY, 1968.
21. J. P. Serre, Propriétés galoisennes des points d'ordre fini des courbes elliptiques, *Invent. Math.* **15** (1972), 259–331.
22. R. Solazzi, The automorphisms of certain subgroups of $PGL_n(V)$, *Illinois J. Math.* **16** (1972), 320–348.
23. Z. X. Wan and H. S. Ren, Automorphisms of linear groups of rank 2 over local rings of characteristic 2, *Chinese Ann. Math. Ser. A* **4**(4) (1983), 419–434.
24. L. Q. Wang, Automorphisms of 2-dimensional linear groups over local rings, *J. Math. Res. Exposition* **5**(1) (1985), 25–28.
25. W. C. Waterhouse, Automorphisms of $GL_n(R)$, *Proc. Amer. Math. Soc.* **79**(3) (1980), 347–351.